CAMERA SURVEILLANCE REGULATIONS VRIJE UNIVERSITEIT AMSTERDAM

Version 1.3

LOOKING FURTHER

Camera Surveillance Regulations Vrije Universiteit Amsterdam

Contents

Introduction

Camera surveillance is carried out on the grounds and in the buildings of Vrije Universiteit Amsterdam (hereinafter: **VU**). The image-based information obtained with this camera surveillance is recorded and stored by digital means. This is a personal data processing operation.

The VU carries out camera surveillance on the legal basis that this serves a legitimate interest of the VU. The use of camera surveillance is a necessary measure for the VU in order to:

- protect the safety and health of its students, employees and visitors on its grounds and in its buildings;
- protect its grounds and buildings;
- protect property located on its grounds and in its buildings; and
- record incidents.

Camera surveillance can intrude on the private life of students, employees and visitors. The VU therefore only makes use of camera surveillance on locations where this is necessary and where less intrusive measures are not effective. These decisions are made on a location-by-location basis and are subject to periodic evaluation.

The purpose of these regulations (hereinafter: **Regulations**) is to promote and ensure that:

- the VU adheres to the applicable laws and regulations on the protection of personal data;
- camera surveillance is used in an ethical manner; and
- students, employees and visitors receive sufficient information about the VU's use of camera surveillance.

The Regulations outline the duties, responsibilities and procedures within the VU and describe how data subjects can exercise their rights.

Article 1. Definitions

The terms used in these Regulations have the meaning as defined in the General Data Protection Regulation and related laws and regulations (hereinafter: the **Law**), unless explicitly stated otherwise.

a. **Images**: the images recorded and retained by the camera system.
b. **Management**: all actions to ensure the continuity of the camera surveillance.
c. **Manager**: the Head of Security of the Campus Services (FCO) of the VU and, in his absence, his deputy.
d. **Data Subject**: the person of whom images are recorded and retained by the camera system. This could be a student, employee or visitor on the grounds and/or in the buildings of the VU.
e. **Authorized Officer**: the person whom the VU has authorized to access the Camera Surveillance equipment under the responsibility of the Manager or Systems Officer for professional purposes. In addition to Employees, this may also include those working at the VU without a contract of employment with the VU, such as temporary employees, seconded employees, self-employed persons or trainees.
f. **Camera Surveillance**: surveillance with the aid of cameras.
g. **Executive Board**: the board of the VU.
h. **FCO Director**: the director of the Campus Services (FCO) of the VU.
i. **Data Protection Officer (DPO)** of the VU: an internal officer within the meaning of Article 37 ff. of the General Data Protection Regulation (AVG). The DPO independently supervises the compliance with data protection laws and regulations and the policies of the VU regarding the protection of personal data.
j. **Incident**: an undesirable event or suspicion of such an event.

k. **Employee**: the person who has a contract of employment with the VU Foundation.
l. **Personal Data**: all information about an identified or identifiable natural person (the Data Subject). Personal Data is a broad term comprising virtually all data relating to a natural person. This includes both objective and subjective data, irrespective of whether the information is correct. It thus comprises information about a person (such as his name, date of birth and gender) as well as value judgements (such as an employee's performance appraisal). Only in exceptional cases does information concerning a natural person not qualify as Personal Data.
m. **Server room**: the room where the server for storing the images obtained via the Camera Surveillance is located.
n. **Systems Officer**: the manager Real Estate (FCO) and, in his absence, his deputy.
n. **Personal Data Processing**: any operation or set of operations which is performed on Personal Data, whether or not by automated means, including in all events the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data**.**

Article 2. Scope

2.1 These Regulations apply to all grounds and buildings where the VU makes use of Camera Surveillance[1] and relates to every Processing of Personal Data based on the Images.
2.2 These Regulations do not apply to grounds and buildings that the VU rents out to third parties. Any Camera Surveillance on these grounds and in these buildings takes place under the responsibility of the tenants.
2.3 These Regulations do not concern the use of cameras during tests and examinations.

Article 3. Purposes

3.1 The VU collects and processes the Images exclusively to:
a. protect the safety and health of students, Employees and other Data Subjects who are on the grounds or in the buildings of the VU;
b. protect access to the grounds and buildings of the VU;
c. protect any property that is located on the grounds and in the buildings of the VU; and
d. record incidents.

Article 4. Responsibility and categorization of duties

4.1 The Executive Board is responsible for the Camera Surveillance.
4.2 The FCO Director is responsible towards the Executive Board for the Camera Surveillance.
4.3 The Manager is responsible for the Management and the supervision of the implementation of the Camera Surveillance and reports on this to the FCO Director.
4.4 The Manager appoints Authorized Officers who are permitted for the purposes mentioned in Article 3 to operate the camera system and view both live and recorded images subject to the conditions set out in these Regulations.
4.5 The Systems Officer is responsible for the technical management of the Camera Surveillance in consultation with the Manager. The Systems Officer appoints Authorized Officers who have access to the Camera Surveillance equipment for servicing and management purposes. Third parties require the permission of the Systems Officer to obtain access to the Camera Surveillance equipment for servicing and management purposes.

[1] This concerns grounds and buildings owned by the VU as well as grounds and buildings rented by the VU.

4.6 All Authorized Officers tasked with Camera Surveillance duties protect the integrity and confidentiality of the images. An Authorized Officer may not use the Images for any other purpose than is necessary for the performance of his duties and is obliged to maintain the confidentiality of all information that comes to his knowledge in the course of his duties.

Article 5. Security

5.1 The VU has taken adequate technical and organizational measures to prevent unauthorized access to the Camera Surveillance equipment as well as the loss or any form of unlawful processing of the Images.
5.2 The physical spaces where live and recorded images can be viewed are accessible to Authorized Officers 24 hours a day and 7 days a week and are protected against burglary and vandalism.
5.3 The Images are stored in encrypted form in a closed system on separate servers. The Server Room is physically protected against unauthorized access. The server rooms are protected against burglary and vandalism.

Article 6. Placement of cameras

6.1 The Manager and Systems Officer jointly decide on the placement of cameras, where necessary in consultation with the FCO Director. Decisions to place a camera are made after careful consideration of the need to protect the Data Subjects' private life versus the interests of the VU.
6.2 Camera surveillance is only used for the purposes set out in these Regulations, at locations where this is necessary and less intrusive measures are not effective. The need for Camera Surveillance at a specific location is evaluated from time to time.
6.3 In rooms where individuals should not be disturbed, such as toilets, showers and dressing rooms, camera surveillance by definition intrudes too much on the private life of the Data Subjects and is not allowed.
6.4 Camera surveillance is not intended to keep track of Data Subjects in the course of their work or visit. Positioning of cameras where Data Subjects are tracked continuously on camera is therefore avoided insofar as possible. At locations where there is an increased security risk of e.g. aggression or theft, Data Subjects may be tracked continuously on camera if this is necessary and less intrusive measures are not effective.
6.5 Signs, stickers and/or screens at the entrances to and exits from the grounds and buildings and at specific locations in the buildings express that Camera Surveillance is in effect. These Regulations are posted on the public website of the VU and intranet (VUnet) to inform Employees, students and other Data Subjects of the purposes of the Camera Surveillance and the conditions governing the processing of their Personal Data.

Article 7. Temporary hidden camera surveillance

7.1 Hidden cameras can be temporarily deployed on the grounds and in the buildings of the VU, but only in exceptional situations. Hidden cameras are never placed in the areas referred to in Article 6.3.
7.2 Hidden cameras are only deployed for the purposes mentioned in Article 3 at locations where this is necessary and less intrusive measures are ineffective. The need for Camera Surveillance at a certain location is periodically evaluated. A hidden camera is only used as a 'last resort' after other solutions have proved ineffective.
7.3 A decision to place a hidden camera rests exclusively with the Executive Board.
7.4 The VU informs the Data Subjects of the use of hidden cameras as soon as these are no longer necessary for the purposes referred to in Article 3.

Article 8. Retention Period

8.1 The Images are retained for a maximum of 10 days after which these are irretrievably erased, unless:
a. the Images relate to an Incident. In this case, the Images are retained until the investigation into or handling of the Incident has been finalized; or
b. a request to access the Images has been submitted in conformity with Article 9.1 and the Images have not yet been erased. In this case the Images are retained until a decision has been made regarding the request for access and – insofar as the request is granted – the Data Subject has had access to the Images.

Article 9. Data Subject Rights

9.1 A Data Subject has a right to access Images on which he is recognizable and if the Images have not yet been erased. The VU can refuse access, for instance if this is necessary for the prevention, detection and prosecution of criminal offences or to protect rights and freedoms of others. A person who suspects he has been recognizably recorded on camera can also request access. In this case, the VU will first check whether the Images contain data of the requester. If this is the case, the request for access will be taken into consideration.

9.2 A Data Subject has the right to erasure of, or restriction of access to, Images on which he is recognizable insofar as his Personal Data have been unlawfully processed or the Personal Data are not or no longer relevant for the purpose for which they were collected.

9.3 A Data Subject has the right to object to the use of his Personal Data by the VU. If the objection is upheld, the VU shall immediately terminate the disputed data processing.

9.4 The requests as referred to in Articles 9.1, 9.2 and 9.3 can be directed to the DPO. This also applies to the exercise of other rights that the Data Subject has on the basis of the Law. The Data Protection Officer of the VU shall notify the Data Subject whether or not the request has been granted as promptly as possible and in any event within no more than four weeks.

9.5 Complaints relating to the use of Camera Surveillance and the behaviour of the Manager or the Authorized Officers can be submitted in writing to the Executive Board. The Executive Board shall respond to the complaint within four weeks.

9.6 The Data Subject can at all times submit a complaint about the Processing of Personal Data to the Dutch Data Protection Authority (AP).

9.7 The Data Subject can at all times turn to the competent court concerning the manner in which Personal Data are processed by the VU.

Article 10. Access to and disclosure of Images

10.1 Access to the Images and disclosure of the Images to third parties only takes place:
a. if demanded by the police or the Public Prosecutor;
b. if a criminal offence or suspicion of a criminal offence is reported; and
c. in other cases where this is compatible with purposes referred to in these Regulations and the Law provides a legal basis for this.

10.2 The Executive Board always checks whether the demand from the police or the Public Prosecutor provides a sufficient legal basis for the requested access and/or disclosure.

10.3 A request for access to and/or disclosure of the Images by third parties who are not Data Subjects must be submitted to the Manager. The Manager shall inform the FCO Director and the Executive Board of this request. The Executive Board shall decide on the request as promptly as possible, taking explicit account of the Data Subjects' right to protection of private life.

10.4 Before receiving access to the Images or a copy of the Images, the party in question must provide proof of identity to the Manager. Access to the Images is provided in the presence of the Manager or an Authorized Officer. The recipient of a copy of the Images must sign for receipt.

Article 11. Final provisions

11.1 The Executive Board shall decide in cases not provided for in these Regulations.
11.2 These Regulations have been submitted to:
a. the VU Staff Council for approval;
b. the VU University Student Council for an opinion.
11.3 These Regulations have been posted on the website of the VU and the intranet (VUnet).

These Regulations have been adopted by the Executive Board and take effect on 24 July 2018.

***